

ABSTRACT

A computer-network security system and method including the steps of providing a deception to a network intruder on the computer-network, monitoring a response of the network intruder to the deception, detecting the network intruder based upon the 5 response of the network intruder to the deception, collecting data regarding the network intruder;, and acting on the data regarding the network intruder to protect the computer-network. This system includes a deception unit, an interception unit, a detection unit, a notification unit, a receiving unit, a database unit, a watching unit and a management unit. Also disclosed are deception methods for protecting a network, and a graphical 10 display system which permits operators to rapidly assess an attack and take corrective action.